

★完全公开



网神 SecFox 日志收集与分析系统 V5.0 产品白皮书

首次创建时间：2023 年 9 月 19 日
最新修改时间：2024 年 10 月 18 日

地址：北京市西城区西直门外南路26号院1号

邮编：100044

● 版权声明

奇安信集团，保留所有权利。

奇安信集团及其关联公司对其发行的或与合作伙伴共同发行的产品享有版权，本文中出现的任何文字叙述、文档格式、插图、照片、方法、过程描述等内容，除另有特别注明外，所有版权均属奇安信集团及其关联公司所有；受各国版权法及国际版权公约的保护。

对于上述版权内容，任何个人、机构未经奇安信集团或其关联公司的书面授权许可，不得以任何方式复制或引用本文的任何片断；超越合理使用范畴、并未经上述公司书面许可的使用行为，奇安信集团或其关联公司均保留追究法律责任的权利。

由于产品版本升级或其它原因，本手册内容会不定期进行更新。除非另有约定，本手册仅作为使用指导，本手册中的所有陈述、信息和建议不构成任何明示或暗示的担保。

● 免责声明

本免责声明（“本声明”）适用于奇安信集团（包括但不限于奇安信科技集团股份有限公司、网神信息技术（北京）股份有限公司、北京网康科技有限公司，以及前述主体直接或者间接控制的法律实体）旗下推出的全部产品和服务（以下统称“本产品”）。如您使用前述产品，即表示您同意接受本声明的一切内容。如果您不同意接受，请立即停止使用相关产品。

奇安信集团有权随时自行决定修改、添加或删除本声明的全部或部分內容。您有责任定期检查免责声明部分的内容，以了解是否发生了变更。如您在我们发布变更后继续使用本产品，即表示您接受并同意这些变更。

1. 您明确理解并同意，本产品按“现状”提供，不存在任何形式的明示或暗示保证，并且在适用法律允许的最大范围内，奇安信集团不提供任何明示或暗示的陈述或保证，包括但不限于有关适销性、适用于特定目的以及不侵犯第三方权利的保证。奇安信集团不保证产品中所含的功能将满足您的全部要求，也不保证您对本产品的使用不会中断或出错。选择本产品来达到预期结果，以及安装、使用本产品并获取结果所带来的所有责任和风险由您承担。
2. 奇安信集团承诺致力于不断提升产品的质量，本产品是在现有技术基础上提供的，但奇安信集团无法保证您使用本产品将完全符合您的期望，包括但不限于不能保证您【通过使用产品能够发现所有的安全漏洞以及能检测到所有的入侵威胁，检测到的入侵威胁不保证完全正确】，您理解并同意，出现前述不符合您对产品期望的情形不视为奇安信集团违约。
3. 您明确理解并同意，您在使用本产品过程中可能发生不可抗力或不可预见的情形，包括但不限于：1)被某些未经许可的个人、团体或机构通过某种渠道获得或篡改；2)因通信繁忙出现延迟，或因其他原因出现中断、停顿或数据不完全、数据错误等情况，从而使交易出现错误、延迟、中断或停顿；3)因地震、火灾、台风及其他各种不可抗力因素引起的停电、网络系统故障、电脑故障等；4)计算机系统可能因存在性能缺陷、质量问题、计算机病毒、硬件故障及其他原因；黑客攻击、计算机病毒侵入或发作等非可归责于奇安信集团的原因；5)政府管制、网络故障、国家政策变化、法律法规之变化等。如发生不可抗力或不可预见的情形，奇安信集团将尽最大努力予以补救，但奇安信集团对于因不可抗力或不可预见的情形造成的各类直接或间接损失，均不承担任何责任。
4. 对于任何本产品的使用行为，包括但不限于您自身和/或任何第三方的行为，奇安信集团均不承担任何责任。
5. 对于从非奇安信集团指定途径以及从非奇安信集团发行的介质上获得的本产品，奇安信集团无法保证其是否感染计算机病毒、是否隐藏有伪装的特洛伊木马程序或者黑客软件。使用此类产品，将可能导致不可预测的风险，建议用户不要轻易下载、安装、使用，奇安信集团不承担任何由此产生的一切法律责任。
6. 上述免责声明适用于因任何性能故障、错误、遗漏、中断、删除、缺陷、操作或传输

延迟、电脑病毒、通信线路故障、失窃、毁坏、未经授权的访问、篡改或使用（无论是出于违约、侵权、疏忽或任何其他诉因）而导致的任何损害、责任或伤害。

7. 奇安信集团保留在不发布通知的情况下随时采取以下行动的权利：在执行常规或非常规维护、错误纠正或其他更改所必需时，中断或修改本产品的任何组成部分的运行或功能。
 8. 本声明受中华人民共和国法律的约束并依据其解释。
 9. 在法律允许的最大范围内，本声明最终解释权归奇安信集团享有。
-

修订记录

版本	状态	修订理由和内容摘要	修订人	批准人	修订日期
V1.0.0	C	新建	刘震		
V1.1.0	A, M	1.3.3 新增 PK03M 型号 修改部分格式	杨威龙		2023/2/23
V1.2	M	“奇安信网神”修改为 “网神”	杨威龙		2023/3/30
V1.3	AM	新增 2.19 数据安全性保护，全文修订	刘震		2023/9/19

状态：C-创建，A-增加，M-修改，D-删除

数据安全分级标注说明

■ 数据分级	公开数据 (Y)	内部数据 ()	普通商秘 ()	核心商秘 ()
<p>*数据分级标注及说明:</p> <ol style="list-style-type: none">1、文档编写前, 应标注数据安全级别, 默认为内部;2、请根据文档内容评估数据安全级别, 在对应数据级别 () 中填写 (Y) ;3、分级 TIPS: <p>【核心商秘】: 限于个别人、小范围共享和使用的信息, 例如薪酬数据、未公开的产生严重危害的样本等。如泄露将导致法律风险或者影响到社会公众利益或者严重的恶意竞争等;</p> <p>【普通商秘】: 限于特定人群、特定范围内共享和使用的信息, 例如公司组织架构、产品样本集等。如泄露存在合规风险或者可能影响社会公众个人利益或者存在一般恶意竞争的风险等;</p> <p>【内部数据】: 限于在公司范围内按需使用, 除去公开数据、核心商秘、普通商秘, 都为内部数据。如泄露不存在法律合规风险或不存在影响社会公众个人利益的风险, 但会产生轻微的恶意竞争风险等;</p> <p>【公开数据】: 对任何方面都无危害的、不会被任何方面进行利用的信息, 例如官网上的产品简介等。如泄露对任何方面都无影响。</p> <p>更多分级 Tips 参考链接: https://sec.qianxin-inc.cn/data-security/data-classification-tips</p>				

目录

1	产品概述	1
1.1	产品简介	1
1.2	产品定位	2
1.3	产品形态及构架	3
1.3.1	产品架构	3
1.3.2	产品形态	3
1.3.3	产品型号与性能	4
2	产品功能	4
2.1	使用模式	4
2.2	审计对象	4
2.3	资产管理功能	5
2.4	日志采集与转发功能	5
2.5	数据治理功能	6
2.6	日志标准化功能	6
2.7	日志过滤和归并功能	7
2.8	事件分析功能	7
2.8.1	事件监视	7
2.8.2	事件统计	8
2.8.3	事件搜索	8
2.9	仪表盘功能	9
2.10	关联分析功能	9
2.11	告警和响应管理功能	10
2.12	报表和报告功能	10
2.13	级联管理	11
2.14	知识库	11
2.15	二次开发接口	11
2.16	系统管理	11
2.17	部署模式	12
2.18	日志备份与恢复功能	12
2.19	数据安全性保护	12
3	特点与优势	13
3.1	全面的采集与数据治理	13
3.2	精准的溯源定位	13
3.3	强大的交互式分析	13
3.4	可弹性扩展的分布式关系分析	14

3.5	丰富的合规模板	15
3.6	丰富的二次开发 API 接口.....	15
3.7	灵活的部署方式	15
4	产品价值	16
4.1	助力网安法和等保合规管理	16
4.2	日常安全策略审计.....	16
4.3	IT 运维好帮手.....	16
4.4	安全分析.....	17
5	应用场景	17
5.1	合规审计.....	17
5.2	安全策略审计.....	18
5.3	攻击与威胁检测	19
5.4	IT 运维与故障排查.....	19
5.5	业务统计分析.....	20
6	安装部署	20
6.1	多平台适配	20
6.2	灵活的部署	21

1 产品概述

1.1 产品简介

当今的政企客户在 IT 信息安全领域面临比以往更为复杂的局面，形势堪忧。这既有来自于企业及组织外部的层出不穷的入侵和攻击，也有来自于组织内部的违规和泄漏。

为了不断应对新的安全挑战，企业和组织先后部署了防病毒系统、防火墙、入侵检测系统、漏洞扫描系统、UTM 等等。这些专业的安全系统都仅仅防堵来自某个方面的安全威胁，形成了一个安全防御孤岛，无法产生协同效应。更为严重地，这些复杂的 IT 资源及其安全检测防御设施在运行过程中不断产生大量的安全日志和事件，这些日志是 IT 运维管理人员和安全管理人員日常运维排查故障的重要依据。它们时刻反映着信息系统内在的真实状况。因此，对日志的分析和管理的管理人员进行安全管理的一个高效和重要的技术手段，它变得日益重要。但它又存在以下几个显著的特征：

1. 来源非常广泛，既包含传统的 IT 环境中各设备和系统产生的日志和告警，又包含移动客户端和传感器产生大量日志；
2. 数量巨大，各种机器和系统时刻产生数据，汇总起来是个天文数量；
3. 种类繁多、格式不统一，各种系统产生的格式不同，含义不同，对人员的专业技术要求不同；
4. 存储分散，不同的日志保存在不同的系统和设备中，收集和阅读需要不同的方法；

以上特点使得日志数据具有典型的大数据特征，如无专业系统，对安全管理人员来说几乎无法处置。安全管理人员面对这些数量巨大、彼此割裂的安全信息，操作着各种产品自身的控制台界面和告警窗口，显得束手无策。人工处理日志数据工作强度大，工作效率极低，难以发现真正的安全隐患。

另一方面，企业和组织日益迫切的信息系统审计和内控、以及不断增强的业务持续性需求，也对当前日志审计提出了严峻的挑战。国家之前实施的信息系统安全等级保护制度（等保 1.0）及当前更新的网络安全等级保护制度（等保 2.0）中，明确要求二级以上的信息系统必须对网络、主机和应用进行安全审计。《中

《中华人民共和国网络安全法》已于 2017 年 6 月 1 日起正式实施。网络安全法正式施行，在网络安全历史上具有里程碑意义，对安全审计提出了新的要求。

综上，企业和组织迫切需要一个全面的、面向企业和组织 IT 资源（信息系统保护环境）的、集中的安全审计平台及系统，这个系统能够收集来自企业和组织 IT 资源中各种设备和应用的安全日志，并进行存储、审计、分析、报警、响应和报告。

网神信息技术（北京）股份有限公司（以下简称“奇安信网神”）借助在安全领域的长期经验积累，结合中国网络安全领域的特殊性，自主研发出了面向中国政企客户的第三代日志审计系统——网神 SecFox 日志收集与分析系统。

网神 SecFox 日志收集与分析系统作为一个统一日志收集与分析平台，能够实时不间断地将企业和组织中来自不同厂商的安全设备、网络设备、主机、操作系统、数据库系统、用户业务系统的日志、警报等信息汇集到审计中心，实现全网综合安全审计。系统能够实时地对采集到的不同类型的日志和事件信息进行标准化（归一化）和实时关联分析，通过统一的仪表盘进行实时动态、可视化的呈现，协助安全管理人员迅速准确地识别安全事故，消除了管理员在多个控制台之间来回切换的烦恼，同时提高工作效率，降低工作强度。

系统为客户提供了丰富的报表模板，使得用户能够从各个角度对企业和组织的安全状况进行审计，并自动、定期地产生报表和报告。用户也能够自定义报表。系统的仪表盘、报表和报告可帮助安全人员对内部管理的合规情况一览无余。

1.2 产品定位

网神 SecFox 日志收集与分析系统 V5.0，真正满足了客户的基于日志的安全审计和安全分析需求，专门为政府、公安、金融、教育、能源、军工、军队、医疗、大中小型企业等用户提供符合《网络安全法》、等保制度、分保制度以及各种行业规范要求的合规性日志审计产品。

1.3 产品形态及构架

1.3.1 产品架构



图 1-1 架构示例图

采集层：采集各种设备和系统的日志和事件，标准化（归一化）为统一的格式，然后进行分类、过滤、归并、补全和丰富；

存储与分析层：数据处理后的日志送入关联分析引擎进行实时的流式关联分析，实时发现安全问题。同时，将日志数据保存至大数据存储中，针对保存的日志数据进行搜索分析、可视化分析、统计分析、合规分析和机器学习等综合分析，发现存在的安全事件。

UI 与功能层：是网神SecFox 日志收集与分析系统的工作界面，用户实现与系统的交互，实现整个系统收集、分析、存储、安全事件告警处置和系统管理的功能。

1.3.2 产品形态

网神 SecFox 日志收集与分析产品具备多种产品形态，提供软件版和硬件版。软件版可根据需要部署在不同的服务器上。硬件版具备多种规格，覆盖低、中、高端产品，覆盖不同日志规模客户。除可服务于全行业客户的基于 x86 架构的产品外，网神 SecFox 日志收集与分析系统还提供了基于信息技术应用创新和国产化平台的产品，满足信创行业和特定行业客户的日志审计的需求。

网神 SecFox 日志收集与分析系统具备多种产品组件，满足客户不同使用场景的使用需求。这些组件包括：日志审计管理中心（又称为主节点）、分布式计算存储节点、分布式日志采集器、网络流量采集器、Windows 日志代理、Linux 日志代理等。其中，日志审计管理中心为必配组件，提供硬件版和软件版两种形态，其余组件为可选组件，除网络流量采集器为硬件形态外，其余组件均为软件形态，部署灵活方便。

1.3.3 产品型号与性能

表 1-1 产品型号规格表

形态	产品型号	综合处理能力	形态	内存	存储	日志保存时间	定位
硬件	LAS-HKH7M	20000EPS	2U 机架设备	32GB	128TB	6 个月 ¹	平台
	LAS-HKO3M	12000EPS	2U 机架设备	32GB	16TB	6 个月 ²	采集器

2 产品功能

网神 SecFox 日志收集与分析系统产品支持SNMP Trap、Syslog、ODBC/JDBC、文件/文件夹、WMI、SFTP、Kafka等多种方式完成日志的收集功能；支持收集各种网络设备（包括但不限于路由器、交换机）、安全设备（包括但不限于防火墙、IDS、IPS、VPN、防病毒网关、网闸、防DDOS攻击、Web应用防火墙）、主机操作系统（包括但不限于Windows、Linux）、数据库（包括但不限于Oracle、Sqlserver、人大金仓）等配置日志、运行日志、告警日志各类型日志；需内置不同统计分析场景，包括各种实时分析场景、历史统计场景、实时统计等。并支持支持自定义分析场景。支持通过柱状图、饼图、折线图等形式的统计信息可视化展示，并可将统计结果保存为报表等；采集服务处理性能达到5000eps及以上；亿条日志查询，请求响应时间≤10秒；每天分析数据量不少于20亿条原始日志，同时系统具备扩展至每天10TB以上的日志分析处理能力，最大支持100TB/天以上数据分析处理能力。

以下简要说明网神 SecFox 日志收集与分析系统产品各组成部分的功能。

2.1 使用模式

网神 SecFox 日志收集与分析系统采用B/S 模式，无需安装客户端，使用 WEB 浏览器访问管理中心，浏览器端无需安装 Java 运行环境。系统支持 chrome 浏览器和 Edge 浏览器。

2.2 审计对象

网神 SecFox 日志收集与分析系统支持审计各种网络设备（路由器、交换机等）配置日志、运行日志、告警日志等；

¹ 平均每秒 1700 条日志入库条件下

² 平均每秒 3000 条日志入库条件下

支持审计各种安全设备（防火墙、IDS、IPS、VPN、防病毒网关，网闸，防DDOS 攻击，Web 应用防火墙、等）配置日志、运行日志、告警日志等；

支持审计各种主机操作系统（包括 Windows\Solaris\Linux\AIX\HP-UX\UNIX\AS400）配置日志、运行日志、告警日志等；

支持审计各种数据库（Oracle、Sqlserver、Mysql、DB2、Sybase、Informix）配置日志、运行日志、告警日志等；

支持审计各种中间件（Tomcat、Apache、Webshpere、Weblogic 等）配置日志、运行日志、告警日志等；

支持各种应用各种应用系统（邮件，Web，FTP，Telnet 等）配置日志、运行日志、告警日志等；

以及用户自己的业务系统的日志、事件、告警等安全信息。

2.3 资产管理功能

网神 SecFox 日志收集与分析系统提供了一个管理各类设备资产的资产库。所有资产都以树形结构进行组织和展示，并能够以此作为权限分配的依据，实现针对资产信息的访问控制，满足资产监控的最小化权限原则。

系统可按照不同的分类方式对组织的 IT 资产进行分组，提供便捷的资产添加、修改、删除、查询与统计、导入、导出功能，便于安全管理和系统管理人员方便地查找所需设备资产的信息。

资产管理可以新增资产标签，扩展资产属性，资产的标签信息及资产属性可作为日志分析时的情景数据，为日志关联分析提供丰富的上下文数据以更加准确的分析威胁和发现攻击。

系统还支持对于 IP 地址的地理信息管理。

2.4 日志采集与转发功能

采集是网神 SecFox 日志收集与分析系统的重要功能，它承载了日志及事件采集、标准化（归一化）、过滤、归并的数据治理功能。采集管理是系统进行日志分析的基础，用户可以通过指定需要采集的目标、采集协议、采集方式进行日

志采集，并对日志源进行管理，监测日志源采集情况、白名单等。系统支持 Syslog、Syslog-NG、SNMP Trap、Netflow 等协议被动采集，支持文件读取、日志代理等方式主动采集、支持 API、JDBC、WMI 等方式交互式采集。支持按照 Syslog-NG 标准及自有格式进行转发，转发时包含原始日志源 IP 地址，系统可转发原始日志或归一化日志，可与 NGSOC、态势感知等产品进行数据对接。

2.5 数据治理功能

无论传统的小数据时代还是大数据时代，数据分析的前提都是高质量的输入数据。否则，大数据分析将变成垃圾数据进垃圾数据出（Garbage In, Garbage Out, GIGO），错误的无法得到正确的结果。因此，为了保证日志分析的准确有效性，日志数据的质量就变得非常重要。系统无法控制被采集对象的日志质量，但可以对采集回来的各种日志进行数据治理。

系统的数据治理主要包括动态数据建模和数据质量管理。动态数据建模为安全审计员提供了一个精细化分析和审计的基础工具。用户可以根据分析和审计的需要构建资产、事件、告警和知识的数据结构模型，这些包括了动态添加资产属性、随时增加事件的属性字段、丰富告警的字段以提供详实的告警信息、完善知识内容。数据质量管理针对数据全生命周期进行质量监测和管理，例如日志采集数量、类型、解析率、关联规则利用率等。

2.6 日志标准化功能

日志标准化又称为范式化或归一化。不同的系统或设备所产生的日志格式是不尽相同的，这给分析和统计带了巨大的麻烦。任何分析都需要在标准化的基础上进行，无论是入库前标准化还是读取时标准化。日志收集后系统对日志进行标准化处理，提取日志属性写入标准化结构的字段中，将机器生成的、人不易理解的内容统一转换为系统可处理、人易读的内容。系统同时对日志进行定级、分类，对内容进行丰富和补全，例如补全资产、地理等属性。系统保留归一化后的日志的同时也保留原始日志，方便用户对原始日志快速定位，便于后期调查和取证。系统提供方便易用的可视化范化工具和智能范化引擎，可对各种日志进行自动化

辅助范化，范化结果所见即所得，系统对采集的日志既可以自动匹配解析策略，也可以人工指定解析策略。智能化的范化技术大幅节省了安全审计人员解析日志和数据处理的工作量，使日志审计变得更简单、更聪明。

系统还支持事件属性字段动态增加，除默认的字段之外，用户可根据自己的审计需要增加字段属性，所有新增的属性字段都可以参与后期的事件查询、关联分析和统计分析。这就使用户在遇到平台内置字段无法满足需求时可以动态扩展字段，大大提升了平台的安全事件分析能力。

2.7 日志过滤和归并功能

系统支持对范化后的日志数据进行过滤和归并。通过过滤和归并，系统可以减并需要存储的日志数量，同时也不影响审计能力。由于对日志进行了标准化，故过滤和归并可以针对单个字段或字段组合进行，这大幅提升了过滤归并的能力。用户可以根据需要设置过滤和归并策略并快速应用。

2.8 事件分析功能

网神 SecFox 日志收集与分析系统提供事件分析功能，用户可以通过界面实时查看来自网络中各种 IT 资源和安全系统的日志情况。网神 SecFox 日志收集与分析系统内置了大量的分析场景，用户无需学习，即可开展审计操作。网神 SecFox 日志收集与分析系统也允许用户自定义场景，并对场景进行树型结构的分类和归档。

2.8.1 事件监视

网神 SecFox 日志收集与分析系统提供强大的事件实时监视和查看功能。系统通过动态时序图和事件列表近实时展示当前网络的动态活动，以及事件分布情况，安全审计人员可以按需实时审计日志，了解特定日志的详细信息和相关的资产等属性，日志可依据策略实时更新和展示。

2.8.2 事件统计

在实时监视过程中，用户可以对关心的事件进行如 IP 地址、事件类型等维度进行统计，分析趋势，对一段时间内的安全事件进行时间切片统计，并描绘趋势曲线。事件以可视化的饼图、柱图、堆积图等方式展现。

系统可对历史日志按照不同的策略进行统计，按照不同的时间周期，如小时/日/周/月/季度/年等进行各种字段和属性日志的统计，并将统计结果以图表的方式进行展现，为不同角色的用户如基层审计运维人员和管理层展现所需的不同内容。系统支持双维度或多维度统计。

2.8.3 事件搜索

网神 SecFox 日志收集与分析系统具备快速的自定义的各种形态搜索。系统为用户提供了一套灵活方便的交互式事件调查工具，通过事件调查工具管理员可以对感兴趣的日志中的重要或全部信息进行查询搜索。

系统提供强大的混合搜索能力，用户不仅可以对固定的日志范化字段进行搜索，也可以通过关键字进行全文检索，将传统基于范化的日志分析和基于全文索引的日志搜索技术完美的结合起来，为安全分析师提供强大的分析工具。

用户可通过查询范化后的字段内容获取到原始日志中不存在的内容信息，这些信息经过范化和丰富，使日志变得更加可读和易于理解，并可快速查询到用户关心的内容，降低了日志审计对用户的专业能力的要求。同时，基于大数据全文索引技术，系统提供了类似搜索引擎的查询能力，用户不需要关注日志是否范化，只需输入关键字后即可即席查询到所有包含关键字的日志。系统支持迭代查询和渐进式分析，通过范化和全文检索的综合使用，分析师可快速发现安全事件和异常，为进一步处置提供基础。

用户可通过交互式查询对比，逐渐收敛事件范围，通过用时间、关键字和复杂流程拼接及迭代嵌套等，发现关联事件和异常事件。

2.9 仪表盘功能

系统提供了灵活自定义的仪表盘，同时内置丰富的仪表盘主题，如：日志源事件分析仪表盘，Windows 事件分析仪表盘，网络设备分析仪表盘，防火墙事件概览分析仪表盘，WEB 事件概览分析仪表盘，FTP 服务器日志分析等，同时用户还可以根据需要进行自定义仪表盘。

通过仪表盘，不同角色和不同用户可快速获取到各自所关注的安全信息，满足各自管理需求。

如概览仪表盘为用户提供了一个从总体上把握企业和组织整体安全情况的界面。通过概览，用户可以快速看到当前企业和组织的整体安全状况。在每个独立的窗口中看到网络中不同维度的实时安全信息，例如事件总量趋势，设备 IP 分布，设备类型分布，事件类型分布，事件严重程度分布，最近 24 小时告警等等。通过这种方式，企业和组织的管理者可以方便地进行全网的安全态势监视。



图 2-1 架构示例图

2.10 关联分析功能

网神 SecFox 日志收集与分析系统提供了强大的关联分析引擎，内置大量关联分析场景，如认证登录、授权行为、违规行为、系统变更、攻击入侵、敏感操作和设备故障等，通过启用这些内置场景规则，可实时发现网络攻击和违规行为。

通过关联分析引擎，用户可以灵活定制关联规则。

关联分析引擎采用可视化编辑方式，用户通过对不同字段的与、或、非等运算符及组合构建复杂关联分析规则，系统支持统计关联、逻辑关联、时序关联等，支持多事件源的关联分析，并可引用规则，多规则嵌套等方式。系统提供活动列表、多种资源表供关联分析规则使用，满足了日志审计的安全场景的分析需求。

系统支持时间窗口关联分析，也支持长周期事件关联分析；既支持实时日志的关联分析，也支持对历史数据的回溯关联分析。

系统将发现的安全事件以告警和事件的方式通知用户，使用户及时了解关联分析的结果。

2.11 告警和响应管理功能

通过关联分析，系统对于发现的安全事件可以进行自动告警，告警内容支持用户自定义字段。告警方式包括邮件、Syslog、SNMP Trap 等。

系统为用户提供了告警列表和统计功能，用户可以按告警 IP 分布、告警等级、告警趋势等维度进行告警浏览，并可查看所有告警详细信息。为了减少重复告警，系统支持基于策略的告警归并和抑制。

告警发生时，系统支持多种响应方式。除了多种通知方式外，用户可对告警进行人工处置，并设置规则自动触发执行自定义的响应方式，如重启应用程序、设备等，控制网络和安全设备进行相应动作等。

2.12 报表和报告功能

系统提供丰富的报表管理功能，预定义了针对各类服务器、网络设备、防火墙、入侵检测系统、防病毒系统、终端安全管理系统、数据库、策略变更、流量，设备事件趋势以及总体报表，满足等保等其他合规性要求，提供自定义报表，用户可根据自身需要进行定制。系统的报表分析引擎能从多种角度多种维度对数据进行分析；能将结果以图形方式（柱图、饼图、曲线图等）显示、打印；报告可用 Word、PDF、HTML、Excel、PNG 等格式存档。

系统还提供了安全运维报告，帮助审计人员生成日常安全运维报告，用户只

需选择报告中集成的数据内容，并手工补充相应的原因分析、解决建议等内容即可快速生成安全运维报告，减轻了审计人员编写日常工作报告的工作量。

2.13 级联管理

提供标准的系统级联，支持对下级系统的注册与注销，可对下级系统的 IP 地址、系统信息、运行状态和性能进行集中监测。

上级指定下级系统进行告警和安全事件数据上报，上级系统可向下级系统下发通知与策略。

2.14 知识库

系统内置安全知识库，包括事件库、案例库、应急预案库、日志采集配置库和端口库等，支持自定义增加安全知识内容。

系统支持 IP 地理位置知识库并支持导入升级。

2.15 二次开发接口

系统提供二次开发接口，接口形式为 Restful API，提供资产、事件、告警、报表等数据的统计、详情等接口；

支持用户认证接口，提供接口在线文档说明供开发人员使用。

2.16 系统管理

采用基于角色的权限管理机制，通过角色定义支持多用户访问；

支持三权分立；内置管理员组与用户组。管理员组包括：系统管理员、安全管理员、审计管理员；用户组默认用户包括：管理员；

支持对于用户登录平台的口令进行强度检查，系统口令错误次数可设置，超过错误次数锁定，锁定时间可设置；

支持双因子认证，作为可选功能，支持国家商密算法的 USB KEY 需单独购买。默认提供用户名口令方式进行身份鉴别；

支持本地用户认证及 Radius 认证；

系统自身的健康状况监控，包括 CPU、内存、磁盘的利用率；

支持页面设置网络接口 IP、网关等信息；

支持页面图形化系统升级；

支持网络诊断工具 Ping, Traceroute, TCPDump 等；

支持分布式部署和级联部署的日志采集器异常告警；

产品内部的各个组件之间通信都支持加密传输，浏览器访问管理中心支持 HTTPS；浏览器支持 session 过期保护，支持超时退出机制；系统具备完善的系统安全策略配置以保证系统。

2.17 部署模式

支持单一部署，也支持分布式集群部署，支持级联部署。

提供分布式日志采集器、分布式计算存储节点，支持水平弹性扩展，由管理中心集中调度管理，提升日志分析和存储性能，分布式计算存储节点支持日志的范化、关联分析、查询和存储。

集群模式下，支持分布式部署，在此部署模式下分布式计算存储节点支持弹性扩容。

2.18 日志备份与恢复功能

系统支持按照日志存储周期进行备份，当磁盘空间日志存储量达到一定百分比时可设定为自动删除磁盘中的历史日志，并进行告警。系统支持日志数据的加密压缩备份，可将日志备份保存至本地存储或外部存储设备中。当需要恢复时，可手动将备份数据进行恢复。外部存储空间的备份与恢复功能为日志审计设备提供了数据的高可靠。

2.19 数据安全性保护

随着《数据安全法》、《国家密码法》、《个人信息保护法》的发布，国家对数据安全的要求越来越高。网神 SecFox 日志收集与分析系统为满足数据安全合规

的要求，特别为满足等保三级以上及关键信息基础设施客户的国家商用密码应用安全性评估（简称密评）测评要求，提供了基于国家商用密码算法的系统关键信息机密性和完整性保护，针对系统采集的日志进行了每条数据的完整性保护，为日志数据提供了签名和验签功能，有效地保护了客户日志数据的完整性和不可篡改性。

3 特点与优势

3.1 全面的采集与数据治理

网神 SecFox 日志收集与分析系统将企业和组织的 IT 资源环境中部署的各类网络或安全设备、安全系统、主机操作系统、数据库以及各种应用系统的日志、事件、告警全部汇集起来，使得用户通过单一的管理控制台对 IT 环境的安全信息（日志）进行统一监控。支持 200 多种设备和系统日志解析，包括了主流的网络设备、安全设备、OS、数据库、应用系统、虚拟化和云计算等，并可不断扩展。

系统提供了丰富的数据治理功能，采用机器学习技术辅助，提供可视化范化能力，使范化更简单，所见即所得。系统可以动态扩展日志属性字段，所有字段均可参与关联分析、查询统计、报表报告等，可以不断扩展审计能力。

3.2 精准的溯源定位

系统内置了全面的全球地理信息库，并支持持续升级。同时，为审计员提供了内网 IP 的地理位置管理，使内外网 IP 的都有了精准的地理位置信息，并自动补充。这一功能可帮助用户准确、高效地定位威胁来源，以地图方式为用户实时动态呈现全球攻击溯源情况。

3.3 强大的交互式分析

网神 SecFox 日志收集与分析系统为安全审计员和分析师提供了强大的交互式分析的平台和工具。这些交互式分析能力包括强大的即席查询，在亿级以上的日志中秒级完成搜索查询，这首先解决了传统基于关系型数据库存储数据搜索慢

甚至不可用的问题，也为安全审计员提供了事件数据探索的平台。系统既支持范
化字段的搜索、也支持原始日志的搜索，还支持范化字段和原始内容的组合查询，
支持迭代查询和回退，也可支持基于策略的查询。

针对查询结果，系统首先进行统计分析，按不同字段进行统计，根据展示效
果生成不同种类的显示图例，包括数值、拓扑图、饼、柱、折线、堆积、地图展
示等。这些图例可以根据分析需要进行任意组合，形成动态仪表盘，为安全管理
人员展示全幅安全场景。仪表盘支持下钻，帮助用户了解安全场景的原始数据。

其次，系统还使用机器学习算法对日志进行分析，帮助用户了解日志结构模
式，快速发现异常日志等。

系统提供了多种可视化分析组件帮助用户对搜索结果进行分析，包括了事件
多维分析、地理分析和关系分析等。事件可视化（Event Visualization）是指
日志审计系统以图形化的方式将标准化（归一化）和关联分析后的事件及其事件
之间的关系形象展示出来的过程，可视化反映出大量事件之间的相互作用关系。
事件可视化是实时的，将安全管理和运维人员从繁重的事件查看工作中解脱出来，
及时直观地进行事件调查，发现安全威胁。系统强大的事件可视化能力，帮助用
户变日常安全管理的认知为感知。

3.4 可弹性扩展的分布式关系分析

网神 SecFox 日志收集与分析系统独有的基于安全监测、告警和响应技术
（Security Monitor, Alert and Response Technology, 简称 SMART）的事件
关联分析引擎。在关联规则的驱动下，SMART™ 事件关联分析引擎能够进行多种
方式的事件关联，包括统计关联、逻辑关联、时序关联、单事件关联、多事件关
联、递归关联等等。具有领先的事件关联分析核心技术，申请了 4 项专利技术，
拥有完全自主知识产权。

系统还独创性的提供了分布式关联分析的能力。传统的集中式关联分析受节
点计算资源的能力限制，在日志的关联分析性能上存在瓶颈，当日志规模超过瓶
颈时，关联分析引擎将无法处理。系统采用了 Map/Reduce 机制的分布式计算技
术，将海量日志的处理分散到集群的计算存储节点中，可通过弹性扩展计算存储
节点数量来增加关联分析的能力，解决了超大规模日志客户的日志关联分析需求。

3.5 丰富的合规模板

内控与合规性审计越来越受到企业和相关监管部门的重视，法规遵从、企业内控成为 IT 业界的热点话题和发展趋势，通过对用户网络环境中安全设备、网络设备、主机、操作系统、数据库系统、用户业务系统等日志进行全面分析与审计，集成各种合规性关键控制点需求，建立基于日志与行为分析的合规性安全审计平台，为用户提供合规性审计报表报告，充分满足各项标准、法规（萨班斯法案、等保要求、分保要求）的合规性控制需求，降低合规性成本。

3.6 丰富的二次开发 API 接口

系统提供了丰富的二次开发接口。用户可以基于二次开发接口与第三方系统进行集成。如通过认证接口进行认证，通过数据接口获取日志审计系统发现的安全违规和攻击威胁等安全告警，获取各类合规统计报表等。实现与第三方系统的不同层级的系统集成。

3.7 灵活的部署方式

网神 SecFox 日志收集与分析系统支持灵活的部署形式，产品形态上分为软件版和硬件版，软件版可以支持物理服务器、虚拟机等多种部署方式，硬件版不同的规格型号满足不同日志处理性能需求。系统支持单机部署、支持分布式采集和集中式关联分析、支持分布式采集和集群式关联分析、支持分布式级联部署方式。

灵活的部署方式使得网神 SecFox 日志收集与分析系统满足了不同规模、不同管理体制的客户的需求。单节点主机可以满足政府企事业单位的小规模客户的审计需求；分布式软件集群部署可以满足超大规模日志客户的集中式审计分析需求；多级级联部署满足了行政管理上具备下级独立审计，上级集中监管的行业客户的需求。

4 产品价值

4.1 助力网安法和等保合规管理

通过部署网神 SecFox 日志收集与分析系统，集中收集客户的 IT 基础设施、应用系统、数据库、安全设备等的日志，进行全面采集、集中存储、关联分析，并针对审计发现的问题进行处置和响应，生成各类合规报表和报告。从而满足网安法对日志保存 180 天的要求和等保 2.0 中二级到四级的安全审计的要求。基于日志的安全审计为客户提供了综合全面的安全审计能力，而不局限在单一数据来源或单一设备。最终，助力客户通过网安法和等保合规检查。

4.2 日常安全策略审计

每个政企客户为了保证组织战略达成，业务可持续发展，必然制定相关的网络安全策略，借助网神 SecFox 日志收集与分析系统，可以实现对组织安全策略的全面审计，了解安全策略的实施情况，从而进行持续改进和完善，提升组织的安全管理水平。系统全面采集客户网络中的各类 IT 基础设施和应用系统的日志，通过对日志的归一化处理，提取安全审计需要的各类属性信息并进行结构化描述。组织的安全审计人员将安全策略转化为系统关联规则（审计规则），系统通过对采集的日志进行实时或历史数据的关联分析，发现组织中的违反安全策略的违规行为和安全事件，结合系统报表和报告，系统可协助安全审计人员出具组织的安全策略审计报告，针对发现的问题进行及时整改，不断完善组织的安全策略。

4.3 IT 运维好帮手

网神 SecFox 日志收集与分析系统，系统可以统一收集各种设备和系统上的日志，并从日志中提取包含时间戳、访问者 IP 地址、行为类别、响应状态等多种信息，当网络出现问题时，IT 可以通过集中分析路由器、防火墙等设备的日志、通过自动化和交互式关联分析快速找到故障的位置和原因。系统可以帮助用户消除各种妨碍运营的合规性约束，它可以为开发人员及应用系统管理员集中提供所有必须的日志文件以方便分析和排查生产故障，而不需要寻求特定的服务器

管理员发送的相应数据资料。因此， 可以作为组织的 IT 运维好帮手，提高 IT 运维人员的工作效率。

4.4 安全分析

安全分析的最佳实践告诉我们， 日志分析是安全分析的最具性价比的方式。网神 SecFox 日志收集与分析系统可以通过集中收集的日志发现来自组织内部和外部的多种安全攻击和威胁事件，并关联分析判断攻击是否成功以及造成的影响。与流量分析、沙箱、蜜罐等共同组成大数据安全分析方案，与工单、各类安全设备等共同组成安全响应和处置方案。

5 应用场景

5.1 合规审计

2017 年 6 月 1 日，《中华人民共和国网络安全法》正式实施，网安法规定，对国家实行网络安全等级保护制度，网络运营者应当按照网络安全等级保护制度的要求，履行安全保护义务，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改。该条第三项明确指出该义务包括“采取监测、记录网络运行状态、网络安全事件的技术措施，并按照规定留存相关的网络日志不少于六个月；”，而《网络安全等级保护基本要求》（等保 2.0）中从二级到四级都明确要求进行日志审计。

网神 SecFox 日志收集与分析系统 V5.0 可最广泛的收集 IT 基础设施和应用系统的日志，包括操作系统、网络设备、安全设备、数据库、中间件、应用系统、虚拟化及云基础设施的日志，它采用大数据的技术可以海量高速、海量的异构日志，并将日志集中存储于分布式非关系型数据库中，支持水平弹性扩展，满足网安法对日志保存 6 个月以上的要求。日志收集与分析系统为了分析日志的需要，对日志进行了结构化描述，同时还将原始日志保存起来，供事后调查取证使用。针对调查取证的需求，系统提供了类似百度、Google 这样的搜索引擎的强大搜索能力，IT 人员通过网络浏览器访问系统后，既可以输入人可以理解的内容进行搜索（这些内容可能不保存在原始日志中，如用户名“张三”，它在原始日志

中可能为“user1, auser”等,设备类型为“防火墙”,日志中可能并不存在“防火墙”字样,它们是在结构化描述时由系统自动添加,方便人理解和系统关联分析),也可以对各种原始日志中的关键字进行搜索,系统就像搜索引擎一样立即给出查询结果。网神 SecFox 日志收集与分析系统采用大数据技术,可在数十亿条日志中秒级返回搜索结果,它使海量日志的调查取证真正变得便捷可用,而不像传统的使用关系型数据库的日志审计系统,在数十亿条日志海量日志中查询到搜索结果可能需要 2-3 个小时,甚至无法返回搜索结果,这对 IT 人员来说是无法忍受并且不可用的。

针对某些国外法规和行业标准,如 Sarbanes-Oxley (萨班斯-奥克斯利法案)、HIPAA 和 PCI-DSS (支付卡行业数据安全标准)标准,日志审计也是满足相关要求的必备技术手段。

5.2 安全策略审计

很多政企行业客户有明确的安全技术策略规范要求,如明确的访问控制策略,如对重要服务器不允许从某部门之外区域进行登录;禁止绕行堡垒机访问系统;对邮件账号的口令长度有明确的要求,如 8 位以上;禁止在服务器上运行某些特定程序;禁止账户给他人使用等。针对这些安全策略的遵从性的检查可以通过日志审计来完成。

网神 SecFox 日志收集与分析系统 V5.0 可采集服务器和部署在服务器上的应用系统的日志,通过审计登录登出日志中的源 IP 地址、登录时间和登录用户等信息进行判断该服务器是否发生了非授权 IP、主机和用户在非授权时间内的访问;针对邮件账号的口令长度,日志分析系统可通过采集 IDS 的检测日志判断是否有低于 8 位字符的口令的邮件账户存在;针对禁止在服务器上运行某些特定程序的审计,日志分析系统可采集服务器上的日志,审计是否存在该程序的运行日志;针对账户借给他人违规使用的情况,日志分析系统可采集相应的登录登出日志,自动化提取登录的时间、源地址和账户信息等,若发现有同一用户同时或短时间内从两个以上相距很远的地点进行登录,则表明其违反了账户管理的安全策略,系统进行报警并进行记录。针对安全策略的审计,日志审计系统结合组织安全策略可轻松胜任,并提供了完整的证据供追溯,从而代替了繁琐的人工审计

过程。

5.3 攻击与威胁检测

网神 SecFox 日志收集与分析系统可以通过集中收集的日志发现来自组织内部和外部的多种安全攻击和威胁事件，并关联分析判断攻击是否成功以及造成的影响。

通过关联分析一段时间内的访问连接日志和 IDS/IPS 等安全设备的日志，网神 SecFox 日志收集与分析系统可以通过集中分析源目的地址相同的大量日志，发现其端口号不同，而且端口号变化较大，结合 IDS 检测到的扫描日志，可发现这是一次来自该源地址的有目的的端口扫描刺探行为。针对该源地址，可通过威胁情报溯源了解该 IP 的具体信息，以辅助管理人员做出相应的决策行为。若系统发现针对该服务器上运行的 Apache 有来自该 IP 的访问行为；且扫描发现其存在 Struts2-045 漏洞，该漏洞是否被攻击者成功利用？在 IDS 等安全设备未更新特征库有效发现攻击者行为之前，日志收集与分析系统通过分析该服务器的用户账户活动信息，发现在扫描刺探攻击之后发生了用户创建的日志，且该用户的角色被赋予管理员角色，这就说明系统发生了被攻击者利用 Struts2-045 的漏洞进行攻陷的安全事件，会及时报警给 IT 管理者。

针对多种安全场景，网神 SecFox 日志收集与分析系统可以通过对日志的集中关联分析实时发现网络中的多种威胁和攻击行为。

5.4 IT 运维与故障排查

日志对 IT 运维和故障排查有非常重要的价值。事实上，syslog 就是为了排障的目的而设计的。在传统运维模式下，组织的运维工程师一旦发现故障，通常会登录到服务器和多个网络设备上，通过字符界面的控制台，用文本处理工具处理日志并查找故障原因。随着网络系统的复杂度增加，分散日志的处理需要逐一登录各台设备，耗时长，效率低，若遇到外部入侵，通常保存在设备和系统上的日志文件可能会被删除，使运维人员无法追溯。

若部署了网神 SecFox 日志收集与分析系统，系统可以统一收集各种设备和

系统上的日志，并从日志中提取包含时间戳、访问者 IP 地址、行为类别、响应状态等多种信息，当网络出现问题时，IT 可以通过集中分析路由器、防火墙等设备的日志、通过自动化和交互式关联分析快速找到故障的位置和原因。如通过分析网络中断日志的时序关系，可以找到引起网络中断的根本原因和起始点。日志收集与分析系统可以快速发现网络设备的电源、板卡和接口等故障情况。

网神 SecFox 日志收集与分析系统可以帮助用户消除各种妨碍运营的合规性约束，它可以为开发人员及应用系统管理员集中提供所有必须的日志文件以方便分析和排查生产故障，而不需要寻求特定的服务器管理员发送的相应数据资料。因此可以以更少的人力快速解决问题，同时不需要访问生产服务器，这样不但不影响生产运营，而且还能满足组织的对服务器的访问的安全合规审计。

5.5 业务统计分析

功能描述政企客户的业务系统的日志可以为客户的业务分析提供依据。网神 SecFox 日志收集与分析系统可以帮助企业客户收集和分析业务系统的日志并进行相应的统计分析。如针对应用系统的访问日志，系统可以针对访问者的源 IP 进行统计分析，可以分析出用户来自哪个地区，不同地区的访问量的大小；可针对访问用户的名称进行统计，可以分析一段时期内活跃用户与非活跃用户；可以统计访问用的浏览器的名称和版本以及所用的操作系统，可以分析用户的操作系统喜好和浏览器的喜好。

6 安装部署

6.1 多平台适配

系统支持灵活的部署方式，具备高弹性部署能力，避免了采用开源大数据技术的重量级资源需求。系统支持水平弹性扩展，通过增减集群节点来实现计算资源的增减。系统对资源的占用灵活，既可以部署在物理服务器中，也可以部署在虚拟机和 Docker 容器中；既支持传统 x86 架构平台部署，也支持非 x86 架构国产化平台部署，满足不同客户的需求。

6.2 灵活的部署

系统支持单机部署、支持分布式采集部署、支持不同组件部署、支持分布式集群部署、支持级联部署等多种部署方式。满足不同数据规模、网络环境和管理层级的需求。



图 6-1 部署示例图